ALIBABA CLOUD

阿里云

数据库审计
用户指南（C100）

文档版本：20220330

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.常用操作导航

由于文档优化调整，本文后期将不再维护并下线，请知悉。

关于使用数据库审计C100的更多信息，请参见用户指南（C100）。

2.授权数据库审计访问云资源

首次使用数据库审计服务前，您需要先完成允许数据库审计服务访问云资源的授权。本文介绍了数据库审计服务关联角色AliyunServiceRoleForDbaudit的权限，如何为数据库审计服务进行云资源授权、以及如何删除服务关联角色。

前提条件

已购买数据库审计C100实例。

背景信息

数据库审计产品在为用户创建和存储用户日志服务SLS的原始日志时，需要获取其他云服务的访问权限，访问控制服务（RAM）会自动创建数据库审计服务关联角色**AliyunServiceRoleForDbaudit**。更多关于服务关联角色的信息，请参见服务关联角色。

应用场景

数据库审计功能需要访问日志服务SLS、专有网络VPC云服务或安全组的资源时，阿里云会自动创建数据库审计服务关联角色**AliyunServiceRoleForDbaudit**，授权数据库审计服务访问其他关联的云服务。

开通访问云资源的授权

操作步骤

1. 登录数据库审计控制台。
2. 在**欢迎使用数据库审计**对话框，单击**授权**。
3. 在**云资源访问授权**页面，单击**同意授权**。

   完成授权操作后，阿里云将自动为您创建数据库审计服务关联角色**AliyunServiceRoleForDbaudit**。您可以在RAM控制台的**角色**页面查看阿里云为数据库审计服务自动创建的服务关联角色。只有创建服务关联角色**AliyunServiceRoleForDbaudit**后，您的数据库审计实例才能访问日志服务SLS、专有网络VPC等云服务的资源。

权限说明

AliyunServiceRoleForDbaudit具备以下访问权限：

- SLS相关资源，具备操作相关的**project**和**logstore**权限。

```
{
    "Version": "1",
    "Statement": [{
            "Action": [
                "log:ListProject"
            ],
            "Resource": "acs:log:*:*:project/*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "log:CreateProject",
                "log:GetProject",
                "log:DeleteProject"
            ],
            "Resource": "acs:log:*:*:project/dbaudit-*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "log:*LogStore*",
                "log:*Index",
                "log:*ConsumerGroup*",
                "log:*SavedSearch",
                "log:*Dashboard"
            ],
            "Resource": "acs:log:*:*:project/dbaudit-*/*",
            "Effect": "Allow"
        }
    ]
}
```

- 专有网络VPC的权限。

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "vpc:DescribeVpcAttribute",
                "vpc:DescribeVSwitchAttributes"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

- 安全组的权限。

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "ecs:DescribeSecurityGroupAttribute",
                "ecs:AuthorizeSecurityGroup",
                "ecs:RevokeSecurityGroup"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

删除AliyunServiceRoleForDbaudit

如果您使用了数据库审计功能，并且需要删除数据库审计服务关联角色**AliyunServiceRoleForDbaudit**，请先释放已有的数据库审计实例，在无数据库审计实例的情况下进行删除。以下介绍删除AliyunServiceRoleForDbaudit的具体操作。

1. 登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 角色**。
3. 在**角色**页面的搜索框中，输入**AliyunServiceRoleForDbaudit**。

   系统会自动搜索到名称为**AliyunServiceRoleForDbaudit**的服务关联角色。
4. 在该角色的**操作**列，单击**删除**。
5. 在**删除RAM角色**对话框，单击**确定**。

常见问题

为什么我的RAM用户无法自动创建数据库审计服务关联角色AliyunServiceRoleForDbaudit？

您需要拥有指定的权限，才能自动创建或删除AliyunServiceRoleForDbaudit。因此，在RAM用户无法自动创建AliyunServiceRoleForDbaudit时，您需为其添加以下权限策略。

```
{
    "Statement": [
        {
            "Action": [
                "ram:CreateServiceLinkedRole"
            ],
            "Resource": "acs:ram:*:主账号ID:role/*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": [
                        "dbaudit.aliyuncs.com"
                    ]
                }
            }
        }
    ],
    "Version": "1"
}
```

3.启用数据库审计实例

购买数据库审计实例后，您需要启用实例，才能登录数据库审计系统并使用审计服务。

操作步骤

1. 登录云盾数据库审计控制台。
2. 在左侧导航栏中，选择**C100实例**。
3. 在**C100实例**页面，定位到需要启用的数据库审计实例，单击**启用**。

> **说明** 只有实例的状态为**未初始化**时，才能执行**启用**。

4. 在**启用**对话框中，选择实例的专有网络和虚拟交换机，并单击**确认**。

> **说明** 专有网络和交换机设置在实例启用后无法修改，请您根据以下情况选择实例的专有网络。
>
> - 审计对象为ECS自建数据库时，选择该ECS所在的专有网络。
> - 审计对象为RDS实例时，选择与RDS实例连接的应用服务器所在的专有网络。

执行结果

在**C100实例**页面，实例的状态更新为**运行中**。

4.管理数据库审计实例的标签

数据库审计提供标签管理功能，方便您标记数据库审计实例资源，实现分类批量管理。本文介绍为实例添加标签、选择已有标签、删除标签等操作。

背景信息

为实例添加新标签

参考以下操作步骤，为数据库审计实例添加标签：

1. 登录云盾数据库审计控制台。
2. 在左侧导航栏中，选择**C100实例**。
3. 在**C100实例**页面，定位到需要添加标签的数据库审计实例。
4. 鼠标移动到实例的**标签**栏图标上，单击**编辑**。

5. 在**标签设置**面板**新建标签**区域中，输入**标签键**和**标签值**，单击**确定**，再单击**确认**。

> **说明** 您可以在标签设置面板中为目标添加多个标签。

新增的标签显示在**标签设置**面板的**标签**区域。

为实例选择已有的标签

参考以下操作步骤，为数据库审计实例选择已有的标签：

1. 登录云盾数据库审计控制台。
2. 在左侧导航栏中，选择**C100实例**。
3. 在**C100实例**页面，定位到需要添加标签的数据库审计实例。
4. 鼠标移动到实例的**标签**栏图标上，单击**编辑**。

5. 在**标签设置**面板**添加标签**区域中，单击已有标签的**标签键**和**标签值**。
   选择的标签会显示在**标签设置**面板的**标签**区域中。
6. 单击**确认**。

通过标签搜索实例

参考以下操作步骤，搜索拥有指定标签的数据库审计实例：

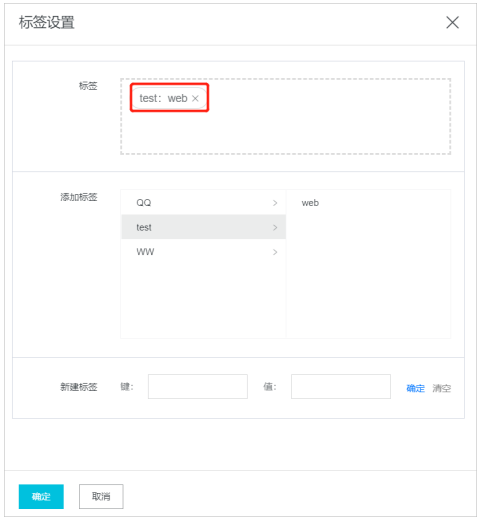
1. 登录云盾数据库审计控制台。
2. 在左侧导航栏中，选择**C100实例**。
3. 在**C100实例**页面的卡片右上方，从标签下拉列表中选择**标签键**和**标签值**。
   符合该标签的实例会显示在**C100实例**页面中。

删除实例的标签

参考以下操作步骤，删除指定数据库审计实例的标签：

1. 登录云盾数据库审计控制台。
2. 在左侧导航栏中，选择**C100实例**。
3. 鼠标移动到实例的**标签**栏图标上，单击**编辑**。

4. 在**标签设置**面板**标签**区域中，单击要移除标签的×图标。



5. 单击**确认**。

> **说明** 数据库审计不支持批量删除多个实例的标签，您只能单独删除某一个实例的标签。

5.管理数据库审计实例

购买数据库审计实例后，您可以在云盾数据库审计管理控制台管理您的数据库审计实例。本文介绍如何为数据库实例配置白名单、管理存储容量、升级和续费。

操作步骤

1. 登录云盾数据库审计控制台。
2. 在左侧导航栏中，选择**C100实例**。
3. 在**C100实例**页面，查看已开通的数据库审计实例的网络、**版本**、**存储信息**、**到期时间**等。

4. 管理数据库审计实例。

   支持对数据库实例进行以下操作：

   - 配置网络白名单

     数据库审计实例开启公网后，您可以单击**配置白名单**，配置可以通过公网访问数据库审计实例的白名单。

   - 升级实例规格

     在**版本**区域，单击**升配**。在**变配**页面，选择需要升级的版本、日志存储容量并选中**数据安全中心服务协议**后，单击**立即购买**。

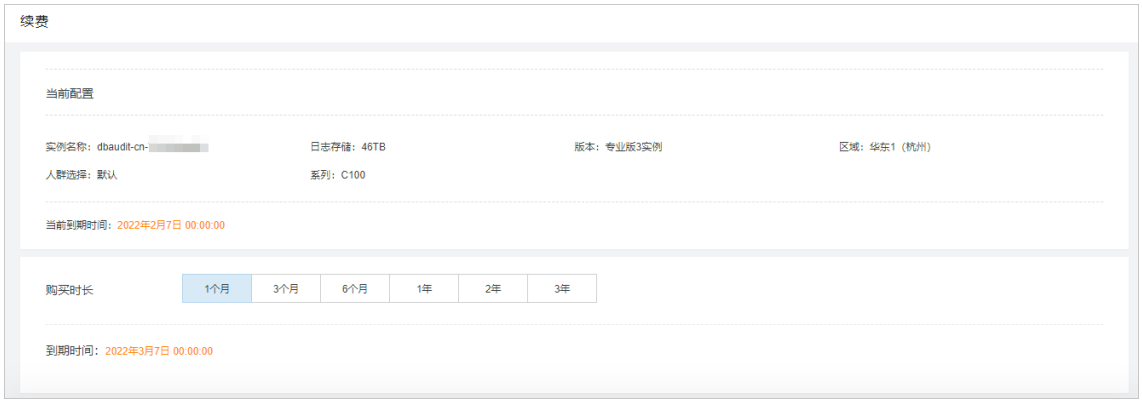
- 存储管理

  在**存储信息**区域，单击**配置**。在**存储管理**对话框，在**审计**或**会话**页签下，您可以清空存储空间、调整存储时长，同时您也可以单击**OSS备份**将您的审计数据或会话记录备份到OSS。

  > **说明**
  > - **存储时长**不能小于30天或大于185天。
  > - **审计（旧版本遗留）**和**会话（旧版本遗留）**页签下的数据为历史版本遗留的数据，您无需关注。

- 续费

  在**到期时间**区域，单击**续费**。在**续费**页面，选择您所需的**购买时长**并选中**数据安全中心服务协议**后，单击**立即购买**完成续费。



> **注意** 数据库审计实例到期后将无法续费，请您关注数据库审计实例的到期时间，并在实例到期前及时续费。

6.登录数据库审计系统

本文介绍了在启用C100数据库审计实例后，登录数据库审计系统的具体操作。

前提条件

已启用C100系列数据库审计实例。具体操作，请参见启用数据库审计实例。

操作步骤

1. 登录云盾数据库审计控制台。
2. 在顶部菜单栏，选择数据库审计实例所在的地域。

3. 在左侧导航栏中，选择**C100实例**。
4. 在**C100实例**页面，定位到要登录的实例， 单击**管理**。

执行结果

成功登录数据库审计系统，进入数据库审计系统的**总览**页面。

后续步骤

完成配置向导。具体操作，请参见C100快速入门。

7.管理数据库资产

在审计数据库前，您必须在数据库审计系统中添加要审计的数据库。已添加的数据库支持编辑和删除操作。本文介绍了在数据库审计系统中添加、编辑、删除数据库的具体操作。

背景信息

关于数据库审计支持的数据库类型，请参见支持的数据库类型。

添加数据库

1. 登录数据库审计系统。

   具体操作，请参见登录数据库审计系统。

2. 在左侧导航栏，选择**资产 > 资产管理**。

3. 在**资产管理**页面，单击**添加**。

> **说明** 您也可以在左侧导航栏单击**总览**，在**总览**页面，单击**资产主要指标**区域的**添加资产**。

4. 在**添加资产**面板，完成数据库配置，并单击**保存**。

配置资产信息时，系统默认为**最简配置**模式（只包含必填项）。您可以单击**更多配置**，切换为更多配置模式（包含必填项和选填项）。

配置项	是否为必填项	说明

配置项	是否为必填项	说明
类型	是	选择要审计的数据库类型和版本。 ○ 如果需要审计的数据库为阿里云数据库，支持选择以下类型： ■ **RDS** ■ **PolarDB** ■ **PolarDB-X** ■ **AnalyticDB** ■ **OceanBase** ○ 如果需要审计的数据库为ECS自建数据库或线下IDC内的数据库，支持选择以下类型： ■ **TiDB** ■ **通用数据库** ■ **大数据** ■ **网站** ■ **其他**
实例名	是	在RDS实例下拉列表中选择要审计的RDS实例ID。 如果还未创建需要审计的RDS云数据库实例，您可以前往RDS管理控制台创建数据库实例。关于创建数据库实例的具体操作，请参见创建RDS MySQL实例、创建RDS PostgreSQL实例、创建RDS SQL Server实例和创建RDS MariaDB实例。 **说明** 只有您将资产类型配置为RDS时，该参数才会显示。
资产组	是	选择要审计的数据库归属的资产组，默认为**缺省资产组**。您可以单击右侧**管理**新增资产组。
名称	是	设置数据库名称。如果选择RDS实例，默认取RDS实例名作为名称，支持修改。
操作系统	是	在下拉列表中选择数据库所在服务器的操作系统类型，支持选择的操作系统类型与数据库类型有关。 **说明** 只有您将资产类型配置为除RDS类型外的其他类型时时，该参数才会显示。

配置项	是否为必填项	说明
编码	否	在下拉列表中选择审计数据的编码类型。支持以下类型： ○ **自动识别**（默认取值） ○ **UTF-8** ○ **UTF-16** ○ **GBK** ○ **ASCII** ○ **ISO-8859-1** ○ **GB2312** ○ **GB13000** ○ **GB18030** ○ **UCS-2** **说明** 如果您不清楚数据库的编码类型，可以先不作修改，保留默认值**自动识别**。当审计的内容不正确或包含乱码时，再使用其它编码类型。
IP端口	是	○ 如果数据库类型选择**RDS**，数据库审计服务会自动获取**IP端口**信息，且不支持修改该信息。 **说明** 成功添加数据库后，您可以修改数据库的IP地址和端口。具体操作，请参见编辑数据库。 ○ 如果数据库类型选择为除**RDS**外的其他类型，您需要手动填写数据库的IP地址和端口。单击**增加IP与端口**可以增加多条记录。 **说明** 在Oracle RAC或MySQL读写分离等场景中，您可以添加多个IP地址和端口，实现对整个集群的审计。
状态	否	设置数据库审计配置状态。支持的状态： ○ **启用** ○ **禁用**
流量方向	否	可以选择**双向审计**或**单向审计**。 ○ 双向审计的审计内容为：请求 + 客户端信息 + 服务端信息 + 返回信息。 ○ 单向审计的审计内容为：请求 + 客户端信息 + 服务端信息。 **说明** RDS类型的数据库默认设置为**双向审计**，且不支持修改。

配置项	是否为必填项	说明
保存行数	否	流量方向为**双向审计**时，设置要保存的返回信息的行数。取值范围：0~999行，0表示不保存返回结果。 流量方向为**单向审计**时，该参数不生效，无需配置。
最大保存长度	否	流量方向为**双向审计**时，设置返回信息的最大保存长度。取值范围：1~64 KB。建议您设置合理的保存长度，避免因长度设置的太小，影响保存的审计结果的完整性。 流量方向为**单向审计**时，该参数不生效，无需配置。
安全证书	否	如果您已为要审计的数据库配置了证书，您需要在此参数处上传数据库正在使用的证书，否则数据库审计服务将无法审计该数据库加密后的访问流量。如果您的数据库未配置证书，则您无需配置该参数。 您可以导入证书或直接复制证书内容到**安全证书**文本框。以下是详细说明： ○ 导入证书：单击**导入**，并选择证书文件上传证书。 仅支持导入PEM格式的证书。如果您的证书为其他格式，您需要先将证书转化为PEM格式再导入。证书格式转化的具体操作，请参见如何转换证书格式？。 ○ 复制证书内容：在**安全证书**文本框，填写证书文件内容的PEM编码。 您可以使用文本编辑工具打开PEM格式的证书文件，复制其中的内容并粘贴到该文本框。 **注意** ○ 您证书使用的算法必须为RSA，否则数据库审计服务将无解析加密后的数据流量。 ○ 您可以联系数据库厂商获取**安全证书**。 配置证书后，数据库审计服务将应用该证书解析加密后的数据库流量并按照您配置的规则审计该数据库的访问流量。
证书密码	否	输入证书的密码。 如果您需要审计的数据库未配置证书或已配置的证书没有密码文件，无需配置此参数。 **注意** 数据库审计服务会妥善保管您的证书密码，该密码经过加密后会被存储在C100数据库实例中，仅在解析当前数据库的加密流量时使用。

> 说明
>
> - 如果需要一次性添加多个数据库资产，您可以在**添加资产**面板顶部选中**保存后不关闭，继续添加数据库**。这样设置后，在完成当前数据库配置并单击**保存**后，可以继续添加下一个数据库。
> - 如果需要为当前数据库启用数据库审计支持的全部内置规则，您可以在**添加资产**面板顶部选中**保存时启用全部内置规则**。您可以在数据库审计控制台**规则配置 > 安全规则**页面，查看数据库审计支持的全部内置规则。
> - 单双向审计配置：添加数据库后，系统默认采用**双向审计**，且审计结果不保存。您可以在**单双向审计配置**区域选用单向或双向审计。只有在选择双向审计时，配置的审计结果保存数量才生效。

成功添加数据库。已添加的数据库显示在**资产管理**页面，您也可以在**总览**页面的**资产主要指标**下查看已添加的数据库。

添加数据库后，您必须在数据库服务器上部署数据库审计的Agent程序，数据库审计服务才能收集目标数据库的访问流量信息。具体操作，请参见安装Agent。同时，您还可以为数据库配置审计规则，使命中规则的审计记录触发告警。具体操作，请参见配置审计规则。

编辑数据库

已添加到数据库审计系统中的数据库配置发生变化时，您需要在数据库审计系统中更新数据库信息。

1. 登录数据库审计系统。

   具体操作，请参见登录数据库审计系统。
2. 在左侧导航栏，选择**资产 > 资产管理**。
3. 定位到要编辑的数据库，单击操作列的**编辑**。
4. 在**编辑资产**面板，修改数据库配置，完成后单击**保存**。

   关于数据库的配置描述，请参见添加数据库的步骤4。

删除数据库

如果不再需要审计某个数据库，您可以在数据库审计系统中将其删除。

1. 登录数据库审计系统。

   具体操作，请参见登录数据库审计系统。
2. 在左侧导航栏，选择**资产 > 资产管理**。
3. 定位到要删除的数据库，单击操作列的**删除**。
4. 在删除提示对话框，单击**确定**。

8.安装Agent

数据库审计系统的Agent程序是部署在用户终端或目标数据库服务器上的功能插件，用来转发数据库访问流量到审计系统。您需要根据数据库服务器的类型，选择合适的方式来安装Agent，才能使数据库审计服务收集目标数据库的访问流量信息。本文介绍安装Agent的具体操作。

Agent程序的安装位置

根据要审计的数据库类型，您需要将Agent程序部署在不同的位置，以下是详细说明：

- 阿里云RDS、PolarDB、PolarDB-X、AnalyticDB和OceanBase数据库

  要审计的数据库为上述阿里巴巴自研数据库时，Agent程序需要部署在与该数据库相连的应用服务器上。阿里巴巴自研数据库中暂时无法安装Agent。

- ECS自建数据库或线下IDC机房中的数据库

  Agent程序可以部署在要审计的数据库所在服务器上，也可以部署在与该数据库相连的Web服务器上。

> 说明
>
> - 如果您要审计的数据库所在ECS使用的是经典网络，您需要先通过ClassicLink功能实现经典网络的ECS与VPC中的数据库审计系统网络互通，然后在ECS服务器上安装Agent。连通经典网络中的ECS和数据库审计系统VPC的具体操作，请参见审计经典网络数据库实例。
> - 如果您要审计的数据库部署在线下IDC机房中，您需要先打通线下IDC机房和数据库审计系统所在VPC的网络连接。您可以通过阿里云高速通道服务打通线上线下的网络连接。

Agent安装方式说明

数据库审计服务支持以下三种安装方式：

安装方式	使用限制	应用场景
通过云助手安装	要安装Agent的服务器需同时满足以下条件： • 已安装云助手的阿里云ECS服务器。 • 和数据库审计实例在同一专有网络（VPC）下。	在ECS服务器上自动批量安装Agent。 在数据库审计系统控制台上一键安装，无需手动下载Agent并安装。
通过SSH远程安装	要安装Agent的服务器需同时满足以下条件： • 操作系统为Linux。 • 支持通过SSH协议登录。	在Linux服务器上批量自动安装Agent。 仅需配置SSH协议相关登录信息，无需手动下载Agent并安装。
下载Agent手动安装	无。	在任意服务器上安装Agent。无法通过云助手安装或通过SSH远程安装时，选择该方式。 使用该方式安装Agent时，需要选择服务器操作系统类型下载对应Agent并手动安装。

通过云助手安装

通过云助手可以一键在云服务器ECS上安装Agent。如果您需要安装Agent的ECS已经安装了Agent，并且该ECS和数据库审计实例在同一专有网络中，推荐您使用该安装方式。以下介绍通过云助手安装Agent的具体操作。

1. 登录数据库审计系统。

   具体操作请参见登录数据库审计系统。
2. 在左侧导航栏，选择**系统管理 > Agent管理**。
3. 在**Agent管理**页面，单击**Agent安装**页签。
4. 在**通过云助手安装**区域，单击**开始安装**。
5. 在**通过云助手安装Agent**对话框中，选中需要安装Agent的ECS实例并单击实例列表上方的**安装**。

   您也可以单击指定ECS实例**操作**列下的**安装**，只为该ECS实例安装Agent。

   安装成功后，对应ECS实例**Agent状态**将变更为**运行中，已连接**。

通过SSH远程安装

数据库审计支持通过SSH协议将Agent安装到您的Linux服务器上。以下介绍通过SSH远程安装的具体操作。

1. 登录数据库审计系统。

   具体操作请参见登录数据库审计系统。
2. 在左侧导航栏，选择**系统管理 > Agent管理**。
3. 在**Agent管理**页面，单击**Agent安装**页签。
4. 在**通过SSH远程安装**区域，单击**开始安装**。
5. 在**通过SSH远程安装Agent**对话框，参考以下参数说明配置要安装Agent的服务器信息。

参数	说明
审计服务器IP	设置数据库审计服务器的IP地址。默认为当前数据库审计实例的服务器IP，您可以根据实际需要修改。

参数	说明
安装Agent的服务器	填写需要安装Agent的服务器的IP地址、账号密码及端口信息，支持选择以下方式填写： ○ **表单填写**：选择该方式时，您需要输入待安装Agent的服务器的IP地址、root账户密码以及端口号。默认端口号为22，您可以根据实际情况修改。 如果需要在多台服务器上安装Agent，单击**增加**并填写服务器信息。 ○ **文本输入**：选择该方式时，您需要按照 `服务器IP,SSH端口,root密码` 的格式输入待安装Agent的服务器的IP地址、端口号以及root账户密码。 不填写密码时，默认使用上一次的密码。 支持IPv4和IPv6格式的IP地址，最多可填写20个服务器的信息。

6. 单击**安装**。
7. 在**安装状态**对话框中，查看Agent的安装状态。

   - 安装成功后，Agent状态将变更为**安装成功**。
   - 安装失败时，Agent状态将变更为**安装失败**。您可以将鼠标移动至**安装失败**右侧的图标，查看安装失败的原因。解决导致安装失败的问题后，您可以单击**操作**列的**重新安装**再次安装Agent。

下载Agent手动安装

您可以通过下载Agent手动安装的方式，在任意需要安装Agent的服务器上安装Agent。以下步骤介绍在Linux和Windows服务器中如何手动安装Agent。

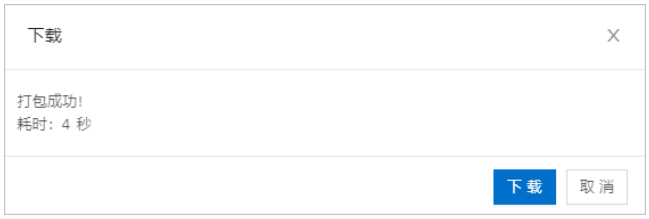
1. 登录数据库审计系统。

   具体操作请参见登录数据库审计系统。
2. 在左侧导航栏，选择**系统管理 > Agent管理**。
3. 在**Agent管理**页面，单击**Agent安装**页签。
4. 在**下载Agent手动安装**区域，根据您的操作系统选择相应版本的Agent安装包并手动安装Agent。

   您需要安装Agent的服务器为Linux服务器时，参考以下步骤操作：

   i. 在**下载Agent手动安装**区域，单击**Linux**。

ii. 等待Agent安装包打包成功后，在**下载**对话框中，单击**下载**。



下载完成后，Agent安装包文件将保存在您浏览器默认的下载路径中。

iii. 登录您的Linux服务器。

iv. 将已下载的Agent安装包上传到Linux服务器的指定目录下。

您可以自定义Agent安装包在Lunix服务器上的存放目录。

v. 执行以下命令，解压Agent安装包。

```
tar -xf dbagent_V1.0.tar.gz
```

> **注意**
>
> - 解压目录中不能出现空格。
> - 每次更换运行或解压目录时，需要重新运行安装脚本。

vi. 执行以下命令，安装并启用Agent。

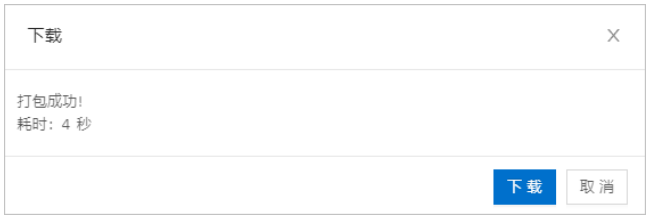
```
./install.sh
```

> **注意**
>
> - 禁止直接运行二进制文件。
> - 必须以root账号运行Agent安装脚本，且指定解释器为bash（或不指定解释器）。

您需要安装Agent的服务器为Windows服务器时，参考以下步骤操作：

i. 在**下载Agent手动安装**区域，单击**Windows**。

ii. 等待Agent安装包打包成功后，在**下载**对话框中，单击**下载**。



下载完成后，Agent安装包文件将保存在您浏览器默认的下载路径中。

iii. 登录您的Windows服务器。

iv. 将已下载的Agent安装包上传到Windows服务器中。

v. 将Agent安装包解压缩到指定的运行目录。

> 注意
>
> - 解压目录中不能出现特殊字符，具体包括：`<space>`、`()`、`[]`、`{}`、`^`、`=`、`;`、`!`、`'`、`+`、`,`、`` ` ``、`~`、`&`。如果一定要在含特殊字符的目录中运行脚本，请以管理员权限进入DOS命令行运行脚本。
> - 每次更换运行或解压目录时，需要重新运行安装脚本。

vi. 进入解压后的Agent安装包的*dbagent > tool*目录，以管理员身份运行**install_npcap.bat**文件安装Npcap工具。

Npcap是运行Agent进行流量代理依赖的工具，需要在安装Agent前完成安装。

vii. 根据Npcap工具安装向导，使用默认配置完成Npcap安装。

viii. Npcap安装完成后，返回*dbagent*目录，以管理员身份运行**install.bat**，安装并启用Agent程序。

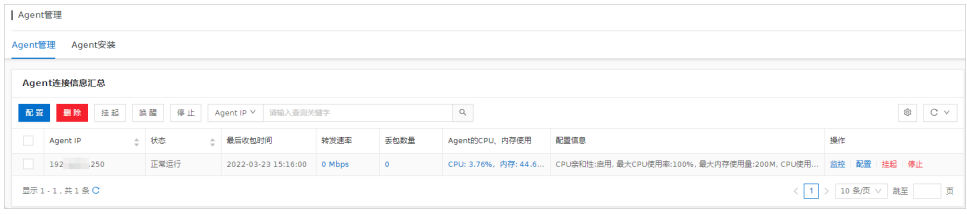
> 注意
>
> - 必须以管理员权限运行Agent安装脚本。
> - 禁止直接运行二进制文件。
> - 如需自行更改配置文件，请勿更改文件的编码格式。

Agent安装完成后，会自动启用。

> 注意 安装过程中遇到问题时，建议您尝试以下方法：等待一段时间后重新安装、卸载Agent并重新安装、重新启动电脑或提交工单联系阿里云技术支持。

5. Agent安装成功后，在**Agent管理**页面，查看Agent连接状态。

Agent的状态为**正常运行**，表示Agent已成功安装并且运行正常。



相关操作

安装Agent后，您可以根据实际需要启用、停用或卸载Agent。请参考以下内容进行操作：

- Linux服务器
  - 卸载：运行安装目录下的uninstall.sh。
  - 启用：运行安装目录下的dbagent_start.sh。
  - 停用：运行安装目录下的dbagent_stop.sh。
- Windows服务器
  - 卸载：运行安装目录下的uninstall.bat。
  - 启用：运行安装目录下的dbagent_start.bat。

- 停用：运行安装目录下的dbagent_stop.bat。

后续步骤

完成Agent安装后，您可以前往数据库审计系统的**总览**页面，查看目标数据库的整体安全状态。

9.审计经典网络数据库实例

如果需要审计经典网络数据库实例，您需要先通过ClassicLink功能实现经典网络的ECS与VPC中的数据库审计系统互通，并在经典网络的ECS上部署Agent程序。

前提条件

VPC中启用ClassicLink时，需要满足限定条件，具体请参见ClassicLink概述的使用限制。

背景信息

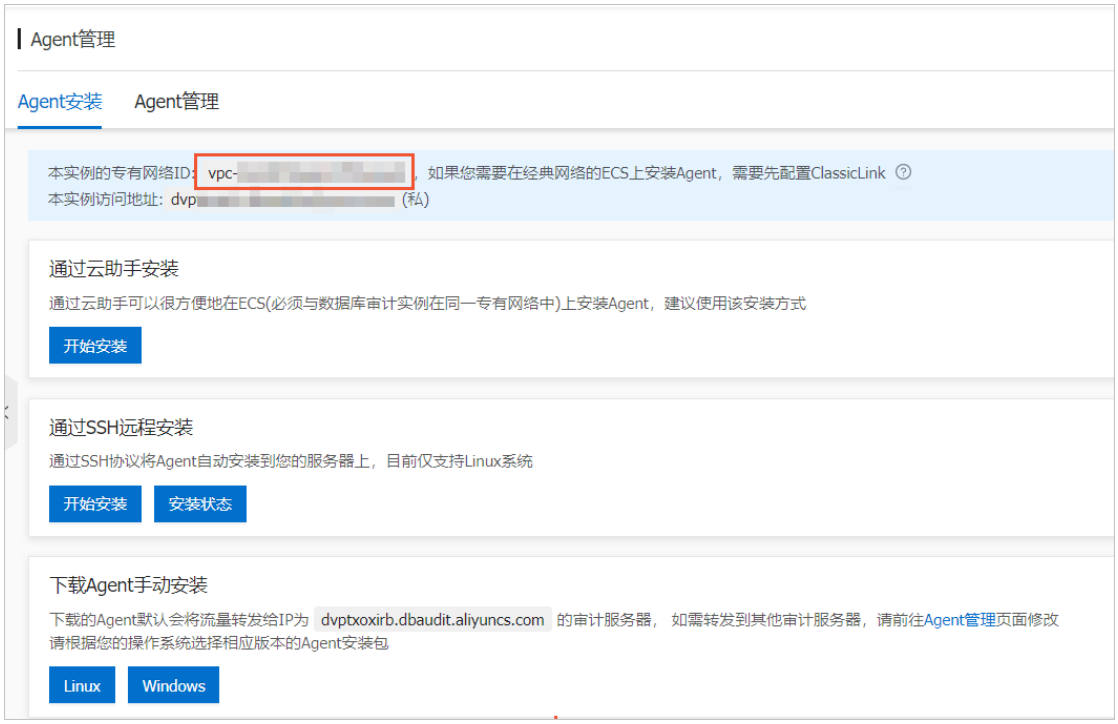
一般情况下，建议ECS和数据库审计系统处于同一VPC中，具体操作请参见安装Agent。

如果您的使用场景比较特殊，ECS需要处于经典网络中，则可以通过ClassicLink功能实现与VPC中的数据库审计系统互通，具体操作请参见本章节。

操作步骤

1. 获取数据库审计系统所在VPC的实例ID。
   i. 登录数据库审计系统。

      具体操作请参见登录数据库审计系统。
   ii. 选择**系统管理 > Agent管理**。
   iii. 单击**Agent安装**页签，查看该数据库审计系统所在的VPC实例ID。



2. 创建经典网络中的ECS实例到数据库审计系统所在VPC的ClassicLink连接。
   i. 在数据库审计系统所在VPC中，开启ClassicLink功能，具体请参见开启ClassicLink功能。

> **说明** 此处操作的VPC实例，请参见步骤1中查看结果。

ii. 在经典网络的ECS中，建立ClassicLink连接，具体请参见建立ClassicLink连接。

在建立ClassicLink连接操作过程中，选择的VPC实例请参见步骤1中查看的结果。

iii. （可选）当VPC网段为192.168.0.0/16时，在经典网络ECS中增加192.168.0.0/16指向私网网卡的路由。

具体操作请参见使用限制。

> **说明** VPC网段为192.168.0.0/16时，需要执行此步骤；VPC网段为其他网段时，不需要执行此步骤。

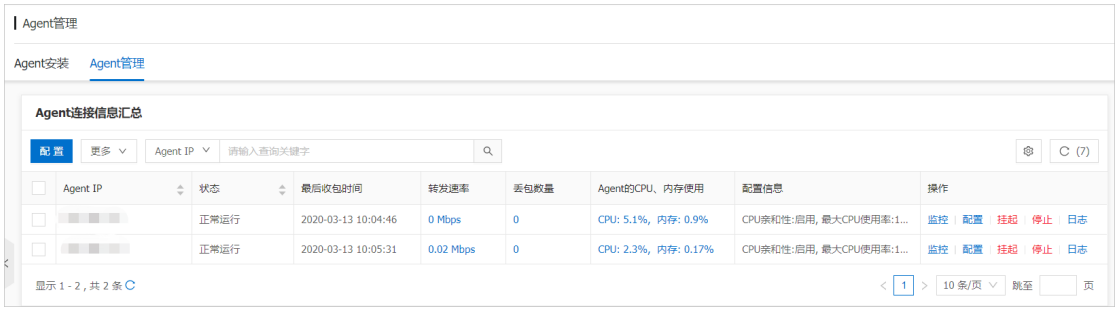
3. 在经典网络的ECS上手动安装数据库审计系统的Agent程序。
   - 如果ECS为Linux系统，具体请参见通过SSH远程安装中**下载Agent手动安装**操作。
   - 如果ECS为Windows系统，具体请参见下载Agent手动安装。
4. 验证是否成功部署Agent程序。
   i. 登录数据库审计系统。

   具体操作请参见登录数据库审计系统。

   ii. 选择**系统管理 > Agent管理**。

   iii. 单击**Agent管理**页签，查看ECS的内网IP是否出现在列表中。

   您如果能够在**Agent IP**列中查看到ECS的内网IP，那么表示连接成功。



后续步骤

Agent程序部署成功后，需要在**资产 > 资产管理**页面配置该数据库的相关信息，配置完成后可在**查询分析 > 审计日志**页面确认是否有审计日志正常入库。

- 配置数据库信息具体操作，请参见管理数据库资产。

- 查看审计日志具体操作，请参见审计日志。

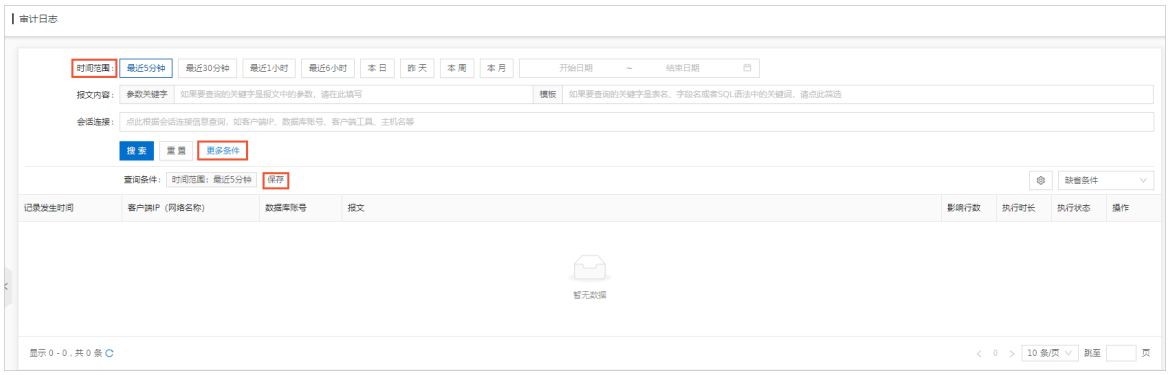
10.查询分析

10.1. 审计日志

通过审计日志，您可以查询所有审计数据。本文介绍了在云盾数据库审计系统中查询审计日志的具体操作。

操作步骤

1. 登录云盾数据库审计系统。具体操作请参见登录数据库审计系统。
2. 在左侧导航栏，单击**查询分析 > 审计日志**。
3. 在**审计日志**页面，设置要查询的**时间范围**和查询条件。

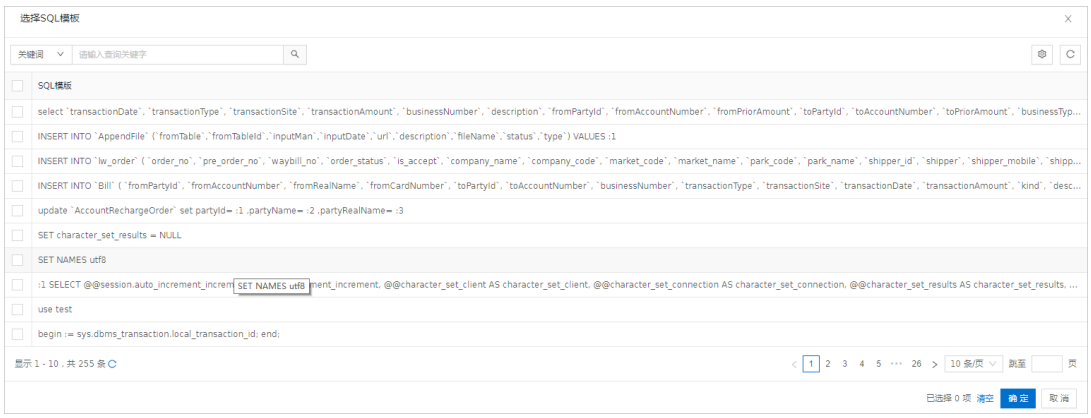


审计查询功能可以帮助您准确定位到具体操作或语句，您可以参考以下步骤来设置查询条件。

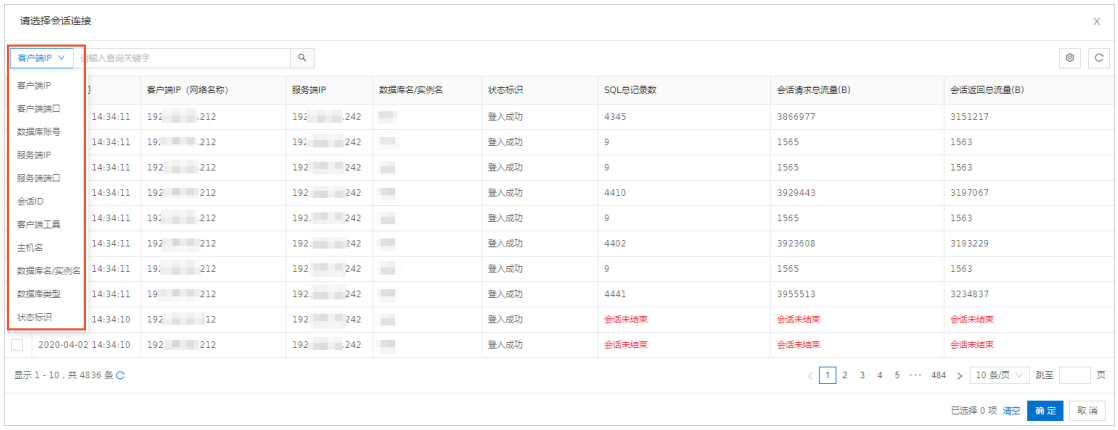
i. 设置**时间范围**。可选择：**最近5分钟**、**最近30分钟**、**最近1小时**、**最近6小时**、**本日**、**昨天**、**本周**、**本月**和自定义。

ii. 设置**报文内容**。

- 如果您要查询的关键字为报文中的参数，那么您可以在**参数关键字**中输入关键字。
- 如果您要查询的关键字是表名、字段名或者SQL语法中的关键词，可以单击模板后的输入框进行筛选，可筛选项包括**关键词**、**SQL模板ID**、**操作类型**。



iii. 设置**会话连接**。可根据会话连接信息进行查询，可筛选项包括：**客户端IP**、**客户端端口**、**数据库账号**、**服务端IP**、**服务端端口**、**会话ID**、**客户端工具**、**主机名**、**数据库类型**、**标识状态**。



iv. 单击**更多条件**可以显示更多筛选条件。可增加的筛选项包括**审计ID**、**数据库名/实例名**、**影响行数**、**执行时长**、**关联IP**、**关联账号**和**执行状态**。

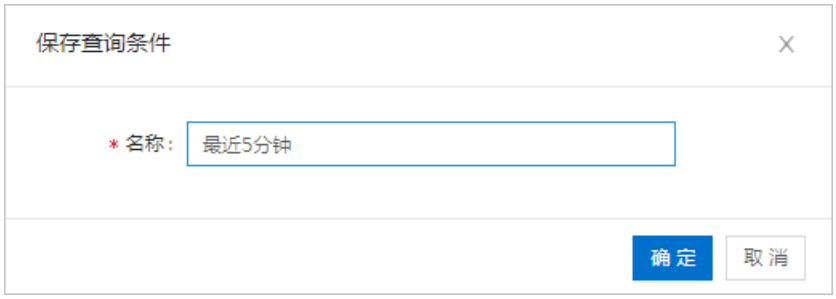
支持的筛选条件见下表。

筛选项	筛选子项	是否默认显示	说明
报文内容-参数关键字	参数关键字	是	关键字是报文中的参数，支持设置多个关键字，多个关键字之间以空格隔开。
报文内容-模板	关键词	否	关键字为表名、字段名或者SQL语法中的关键词。
	SQL模板ID	否	要查询的SQL模板的ID。
	操作类型	否	SQL的操作类型。 包含Select、Insert、Update等操作类型。
	客户端IP	否	需要连接数据库的客户端的IP地址，支持设置IPv4或IPv6地址。
	客户端端口	否	需要连接数据库的客户端的端口号。
	数据库账号	否	登录到数据库的账号名称。
	服务端IP	否	数据库服务器服务端的IP地址，支持设置IPv4或IPv6地址。

筛选项	筛选子项	是否默认显示	说明
会话连接	服务端端口	否	数据库服务器服务端的端口号。
	会话ID	否	要查询的会话ID。
	客户端工具	否	登录数据库的客户端工具。
	主机名	否	数据库服务器的主机名。
	数据库名/实例名	否	数据库名称或实例名称。
	数据库类型	否	数据库的类型。
	标识状态	否	SQL的执行结果，取值如下： ■ 未知 ■ 登入成功 ■ 登入失败
影响行数	影响行数	是	SQL的影响行数。
执行时长	执行时长	是	SQL的执行时长。
执行状态	执行状态	是	SQL的执行结果，取值如下： ■ 全部（默认取值） ■ 未知 ■ 执行成功 ■ 执行失败
审计ID	审计ID	否	要查询的审计ID。输入多个值时请使用逗号（,）隔开。
数据库名/实例名	数据库名/实例名	否	数据库名称或实例名称。

说明 不同设置条件之间为与的关系。

4. （可选）设置查询条件后，单击**保存**，可以保存查询条件。

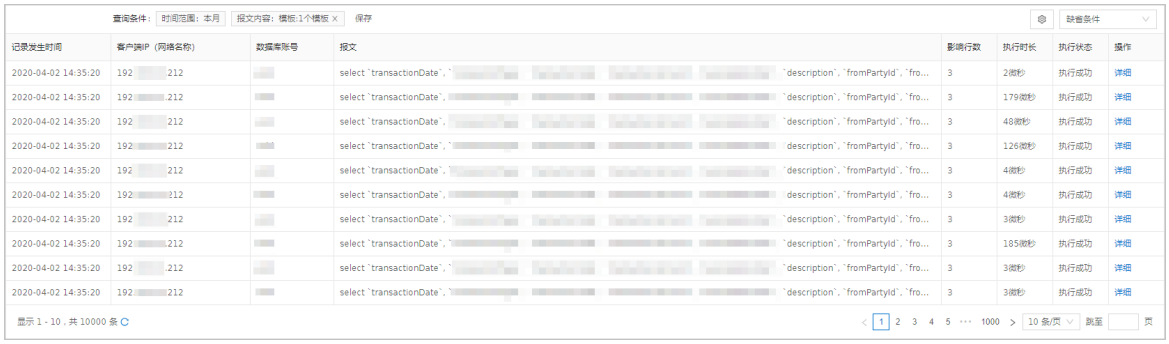


保存查询条件后，如果您后续需要使用相同查询条件，不需要重新设置，可以直接在查询条件下拉列表中选择。

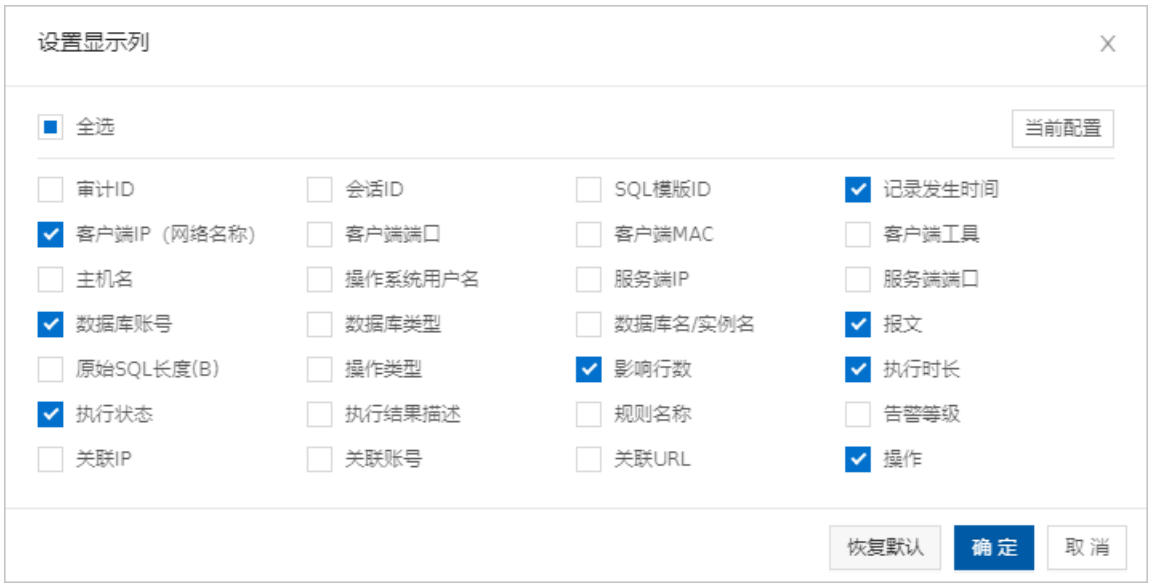
5. 单击**搜索**，执行查询。

> **说明** 一次查询最多可查询10,000条记录。

完成查询后，在**审计日志**页面下方查看返回记录。



6. （可选）您可以单击**设置显示列**图标，并在**设置显示列**对话框中选中要在返回结果中显示的列选项。



10.2. 告警日志

本文介绍了在云盾数据库审计系统中查询告警日志的具体操作。通过告警日志，您可以查询数据库的告警信息。

操作步骤

1. 登录云盾数据库审计系统。具体操作，请参见登录数据库审计系统。
2. 在左侧导航栏，单击**查询分析 > 告警日志**。
3. 在**告警日志**页面，设置要查询的**时间范围**和查询条件。

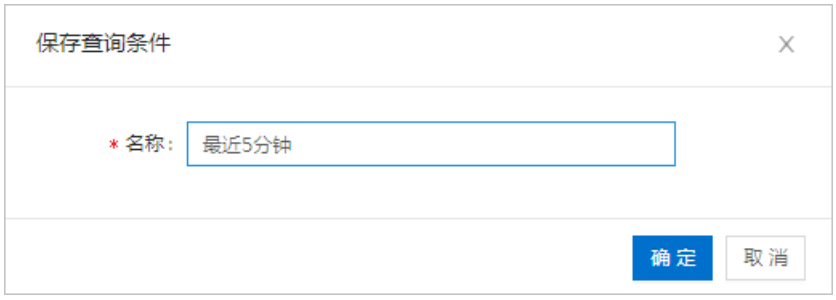
- 时间范围取值：最近5分钟、最近30分钟、最近1小时、最近6小时、本日、本周、本月、自定义。
- 通过设置筛选条件查询相关记录。

告警日志页面上，默认显示了几个常用的筛选条件，如需设置更多筛选条件，可单击**更多条件**选中并设置更多筛选条件。支持的筛选条件说明如下表所示。

筛选项	说明
资产	要查询的数据库。
规则名称	命中的规则名称。

筛选项	说明
告警等级	触发的告警等级。
数据库账号	登录到数据库的账号名称。
客户端IP	客户端的IP地址，支持查询IPv4或IPv6地址。
服务端IP	服务端的IP地址，支持查询IPv4或IPv6地址。
审计ID	要查询的审计ID。
会话ID	要查询的会话ID。
SQL模板ID	要查询的SQL模板ID。
客户端端口	客户端的端口号。
服务端端口	服务端的端口号。
数据库名/实例名	数据库名称或实例名称。
客户端工具	登录数据库的客户端工具。
主机名	数据库服务器的主机名。
影响行数	SQL的影响行数。
执行时长	SQL的执行时长。
操作类型	SQL的操作类型。
执行状态	SQL的执行结果，取值： ■ 全部（默认） ■ 执行成功 ■ 执行失败
数据库类型	数据库的类型。

设置查询条件后，单击**保存**，可以保存查询条件。



已保存的查询条件可以在查询条件下拉框中直接调用。

4. 单击**搜索**，执行查询。

> **说明** 一次查询最多可查询10,000条记录。

5. 在**告警日志**页面下方查看返回记录。

   您可以单击右侧 ⚙ 图标，并在**设置显示列**对话框中选中要在返回结果中显示的列选项。

后续步骤

配置审计规则

10.3. 会话日志

本文介绍了在云盾数据库审计系统中查询会话日志的具体操作。通过会话日志，您可以查询客户端与服务器端之间建立的会话信息。

操作步骤

1. 登录云盾数据库审计系统。具体操作，请参见登录数据库审计系统。
2. 在左侧导航栏，选择**查询分析 > 会话日志**。
3. 在**会话日志**页面，设置要查询的**时间范围**和查询条件。

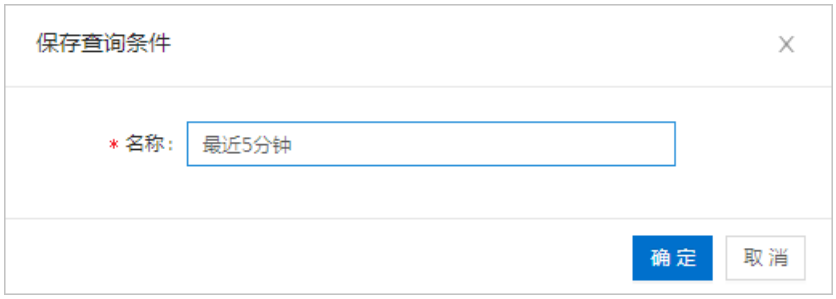
- 时间范围取值：最近5分钟、最近30分钟、最近1小时、最近6小时、本日、本周、本月、自定义。
- 通过设置筛选条件查询相关记录。单击**更多条件**可以显示更多筛选条件。

支持的筛选条件见下表。

筛选项	是否默认显示	说明
资产	是	要查询的数据库。
数据库账号	是	登录到数据库的账号名称。
客户端IP	是	客户端的IP地址，支持查询IPv4或IPv6地址。
服务端IP	是	服务端的IP地址，支持查询IPv4或IPv6地址。
会话ID	否	要查询的会话ID。
客户端端口	是	客户端的端口号。
服务端端口	是	服务端的端口号。
数据库名/实例名	否	数据库名称或实例名称。
客户端工具	否	登录数据库的客户端工具。
主机名	否	数据库服务器的主机名。
数据库类型	否	数据库的类型。

筛选项	是否默认显示	说明
状态标识	否	会话状态，取值： ■ 全部 ■ 未知 ■ 登入成功 ■ 登入失败

- 设置查询条件后，单击**保存**，可以保存查询条件。



已保存的查询条件可以在查询条件下拉框中直接调用。

4. 单击**搜索**，执行查询。

> 说明 一次查询最多可查询10,000条记录。

5. 在**会话日志**页面下方查看返回记录。

您可以单击**设置显示列**图标，并在**设置显示列**对话框中选中要在返回结果中显示的列选项。


设置显示列
缺省条件
设置显示列
全选
当前配置
审计ID
会话ID
SQL模版ID
记录发生时间
客户端IP
客户端端口
客户端MAC
客户端工具
主机名
操作系统用户名
服务端IP
服务端端口
服务端MAC
数据库账号
数据库类型
数据库名/实例名
报文
原始SQL长度(B)
操作类型
影响行数
执行时长
执行状态
执行结果描述
规则名称
告警等级
是否为统计规则
操作
确 定
恢复默认
取 消

后续步骤

配置审计规则

11.规则配置

11.1. 配置审计规则

本文介绍了在云盾数据库审计系统中为数据库配置审计规则的具体操作。

前提条件

已添加数据库。关于添加数据库的具体操作，请参见添加数据库。

背景信息

将数据库添加到数据库审计系统后，您可以为数据库配置审计规则。当审计记录命中配置并启用的审计规则时，审计规则会触发告警。

审计规则包括系统规则和用户规则。

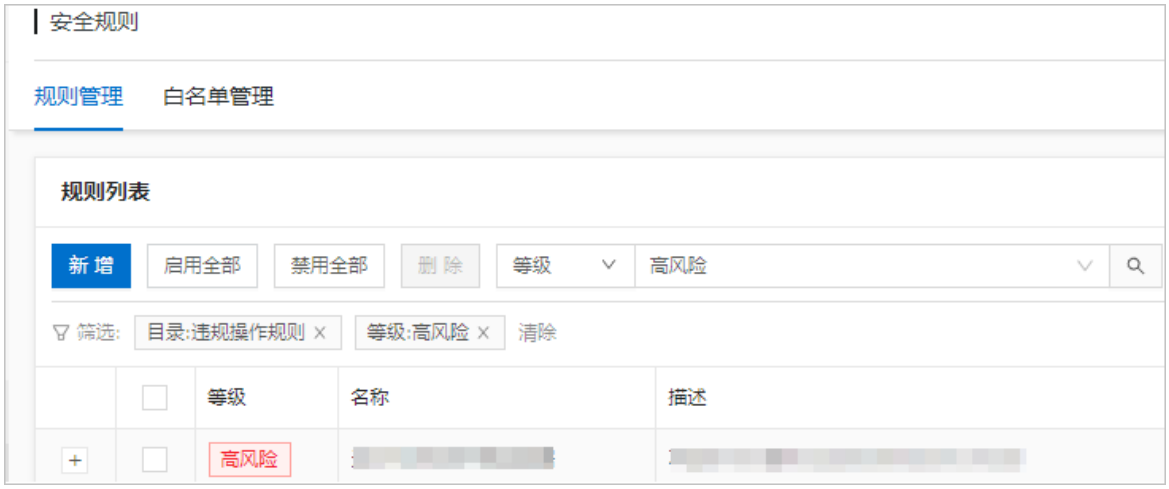
- 系统规则为内置规则，支持的规则类型包括：SQL注入规则、漏洞攻击规则、账号安全规则、数据泄露规则、违规操作规则。每种类型下包括多条规则。不同的数据库支持的系统规则不同，具体以数据库的**规则配置**页面的可使用规则为准。您在添加资产时可以选择是否启用系统规则。
- 用户规则为自定义规则。添加数据库后，您可以为其添加用户规则，用户规则在数据库之间互不通用。

新增用户规则

1. 登录云盾数据库审计系统。

   具体操作，请参见登录数据库审计系统。

2. 在左侧导航栏，选择**规则配置 > 安全规则**。
3. 单击**规则管理**页签。



4. 单击**新增**，在**新增规则**面板，根据面板提示完成规则配置，并单击**保存**。

等级：高风险 中风险 低风险

上级目录：缺省规则组

规则类型：普通规则 统计规则

统计时长：10 秒

允许范围10秒到30分钟

累计次数：2 次

允许范围2到30次

累计条件：同一会话

客户端

客户端来源：IP IP组

等于

可配多个IP，使用逗号“,”分隔，例：192.168.1.2,192.168.1.3

客户端工具：等于

可配多个客户端工具，使用逗号“,”分隔，例：db2bp.exe,javaw.exe,plsqldev.exe

客户端端口：

可配置多个值或区间，多个值间以逗号“,”分隔，例：10-15,20,25,30-40

客户端MAC地址：等于

可填多值，多个值间以逗号“,”分隔，例：fe:58:c0:39:dd:cf,fe:58:c0:55:dd:cf

操作系统用户：等于

可填多值，多个值间以逗号“,”分隔，例：xxx,yyy

主机名：等于

可填多值，多个值间以逗号“,”分隔，例：xxx,yyy

应用IP：IP IP组

等于

可配多个IP，使用逗号“,”分隔，例：192.168.1.2,192.168.1.3

应用用户名：自定义 分组选择

等于

可填多值，多个值间以逗号“,”分隔，例：xxx,yyy

服务端

服务端IP：等于

可配多个IP，使用逗号“,”分隔，例：192.168.1.2,192.168.1.3

服务端端口：

可配置多个值或区间，多个值间以逗号“,”分隔，例：10-15,20,25,30-40

数据库账号：自定义 分组选择

等于

可填多值，多个值间以逗号“,”分隔，例：xxx,yyy

服务端MAC地址：等于

可填多值，多个值间以逗号“,”分隔，例：fe:58:c0:39:dd:cf,fe:58:c0:55:dd:cf


数据库名(SID)：
Oracle数据库输入SID，其他数据库输入数据库名，可填多值，多个值间以逗号“,”分隔
行为
对象组：
包含任一对象则满足
操作类型：
常用值
SQL模板ID：
请输入SQL模板的ID，可填多值，多个值间以逗号“,”分隔
SQL关键字：
1
支持正则表达式
正则校验
添加条件
条件运算逻辑表达式
表达式支持“与、或、非、括号”运算(&：与，|：或，~：非)，条件使用序号表示，即“1”表示条件1，例：~(1&(~3|2))
SQL长度：
大于等于
B
允许范围1B到64KB
关联表数：
大于等于
SQL操作涉及表的个数大于等于此值时触发本规则，允许输入最大值为255
WHERE子句：
不判断
有WHERE子句
没有WHERE子句
结果
执行时长：
大于等于
最小值
秒
允许配置从0到半个小时之间的任意范围，SQL执行时长属于此范围，则触发规则
影响行数：
大于等于
最小值
单位：行，允许配置从0到999999999之间的任意范围。SQL操作返回的记录数或受影响的行数属于此范围，则触发规则
返回结果集：
1
支持正则表达式
正则校验
添加条件
条件运算逻辑表达式
表达式支持“与、或、非、括号”运算(&：与，|：或，~：非)，条件使用序号表示，即“1”表示条件1，例：~(1&(~3|2))
执行状态：
全部
成功
失败
执行结果描述：
匹配
关键字
关键字支持正则表达式格式
其他
生效时间：
自定义
分组选择
任意时间
每天
每周
每月
保存
取消

类别	配置项	支持的逻辑符	说明
基本信息	**名称**	不涉及	规则名称。 **注意** 同一数据库下的所有用户规则的名称不允许重复。
	描述	不涉及	规则描述信息。
	等级	不涉及	命中规则后触发的告警等级。取值：**高风险**、**中风险**、**低风险**。
	上级目录	不涉及	规则隶属的上级目录。
	规则类型	不涉及	规则所属的类型。 取值：**普通规则**、**统计规则**。
	统计时长 **注意** 仅适用于统计规则。	不涉及	统计规则在统计时间内的时长。允许范围10秒到30分钟。
	累计次数 **注意** 仅适用于统计规则。	不涉及	统计规则在时间范围内所触发的统计规则次数。允许范围2到30次。
	累计条件 **注意** 仅适用于统计规则。	不涉及	统计规则可设置的统计条件。取值：**同一会话**、**同一客户端IP**、**同一数据库账号**、**同一客户端工具**。
	客户端来源	**等于**、**不等于**	客户端的IP地址，支持**IP**和**IP分组**。支持填写多个值，多个值之间以半角逗号（,）分隔。例如，192.168.1.2,192.168.1.3。
	客户端工具	**等于**、**不等于**	客户端使用的工具名称。支持填写多个值，多个值之间以半角逗号（,）分隔。例如，db2bp.exe,javaw.exe,plsqldev.exe。
	客户端端口	不涉及	客户端的访问端口号。支持填写多个值或区间，多个值之间以半角逗号（,）分隔。例如，10-15,20,25,30-40。

类别	配置项	支持的逻辑符	说明
客户端	**客户端MAC地址**	**等于、不等于**	客户端机器的MAC地址。支持填写多个值，多个值之间以半角逗号（,）分隔。例如，fe:58:c0:39:dd:cf,fe:58:c0:55:dd:cf。
	操作系统用户	**等于、不等于**	客户端操作系统的登录用户名。支持填写多个值，多个值之间以半角逗号（,）分隔。例如，xxx,yyy。
	主机名	**等于、不等于**	客户端的主机名。支持填写多个值，多个值之间以半角逗号（,）分隔。例如，xxx,yyy。
	应用IP	**等于、不等于**	客户端的IP地址，支持**IP**和**IP分组**。支持填写多个值，多个值之间以半角逗号（,）分隔。例如，192.168.1.2,192.168.1.3。
	应用用户名	**等于、不等于**	客户端的应用用户名，支持**自定义**和**分组选择**。支持填写多个值，多个值之间以半角逗号（,）分隔。例如，xxx,yyy。
服务端	**服务端IP**	**等于、不等于**	服务端的IP地址。支持填写多个值，多个值之间以半角逗号（,）分隔。例如，192.168.1.2,192.168.1.3。
	服务端端口	不涉及	服务端的端口号。支持填写多个值或区间，多个值之间以半角逗号（,）分隔。例如，10-15,20,25,30-40。
	数据库账号	**等于、不等于**	数据库的登录用户名，支持**自定义**和**分组选择**。支持填写多个值，多个值之间以半角逗号（,）分隔。例如，system,sys。
	服务端MAC地址	**等于、不等于**	服务端机器的MAC地址。支持填写多个值，多个值之间以半角逗号（,）分隔。例如，fe:58:c0:39:dd:cf,fe:58:c0:55:dd:cf。
	数据库名（SID）	不涉及	服务端的数据库名。Oracle数据库输入SID，其他数据库输入数据库名称。支持填写多个值，多个值之间以半角逗号（,）分隔。
	对象组	不涉及	SQL语句所属的对象组。支持**包含任一对象则满足**、**包含所有对象才满足**。
	操作类型	不涉及	对数据库的操作类型，取值： ○ **DDL**：Truncate、Create、Alter、Drop、Comment、Rename ○ **DML**：Select、Insert、Update、Delete、Call、Explain、Lock、Merge ○ **DCL**：Grant、Revoke
	SQL模板ID	不涉及	SQL模板的ID。支持填写多个值，多个值之间以半角逗号（,）分隔。

类别	配置项	支持的逻辑符	说明
行为	**SQL关键字**	不涉及	配置方式如下： i. 添加条件。 在条件框中输入要匹配的报文内容，支持使用正则表达式。单击**添加条件**可以添加多个条件。 添加一个条件后，您可以执行**正则校验**，验证指定的内容是否与设置的正则表达式相匹配。操作步骤如下： a. 单击条件下的**正则校验**。 b. 在**正则校验**对话框中，确认**正则表达式**，并输入**校验的内容**。 c. 单击**校验**。 ii. 编写**条件运算逻辑表达式**。 通过与（&）、或（|）、非（~）和括号描述条件间的组合运算关系，条件使用序号表示，例如，“1”表示条件1。 示例： 1&2，表示有两个SQL关键字条件，且两个关键字都要满足，才命中规则并触发告警。
	SQL长度	**大于等于**	SQL语句的长度。允许的范围为1字节到65536字节。
	关联表数	**大于等于**	SQL操作关联表的个数。SQL操作涉及表的个数大于等于此值时触发本规则，允许输入最大值为255。
	WHERE子句	不涉及	是否包含WHERE子句。取值：**不判断**、**有WHERE子句**、**没有WHERE子句**。
	执行时长	**大于等于**、**小于等于**、**区间**	SQL语句的执行时长。单位取值：**秒**、**毫秒**、**微秒**。取值范围为0~2147483647。SQL语句的执行时长属于此范围，则命中规则。
	影响行数	**大于等于**、**小于等于**、**区间**	SQL语句的影响行数。取值范围为0~999999999。SQL操作返回的记录数或受影响的行数属于此范围，则命中规则。

类别	配置项	支持的逻辑符	说明
结果	**返回结果集**	不涉及	配置方式如下： i. 添加条件。 在条件框中输入要匹配的报文内容，支持使用正则表达式。单击**添加条件**可以添加多个条件。 添加一个条件后，您可以执行**正则校验**，验证指定的内容是否与设置的正则表达式相匹配。操作步骤如下： a. 单击条件下的**正则校验**。 b. 在**正则校验**对话框中，确认**正则表达式**，并输入**校验的内容**。 c. 单击**校验**。 ii. 编写**条件运算逻辑表达式**。 通过与（&）、或（|）、非（~）和括号描述条件间的组合运算关系，条件使用序号表示，例如，“1”表示条件1。 示例： 1&2，表示有两个SQL关键字条件，且两个关键字都要满足，才命中规则并触发告警。
	执行状态	不涉及	执行结果中包含的执行状态。取值：**全部**、**成功**、**失败**。
	执行结果描述	**匹配**、**不匹配**	执行结果中包含的关键词，支持以正则表达式的方式进行匹配。
其他	**生效时间**	不涉及	规则的生效周期，支持**自定义**和**分组选择**。取值：**任意时间**、**每天**、**每周**、**每月**。

成功添加用户规则后，您可以在规则列表中查看新添加的用户规则。新添加的用户规则默认无数据库使用该规则（**资产数量**为**0**），您可查看下列启用规则的操作步骤，为数据库引用用户规则。

启用规则

启用规则包括：单独启用规则、批量启用规则、启用全部规则。

单独启用规则，操作步骤如下：

1. 在**规则管理**页面，定位到目标规则，单击**资产数量**列下的数字。

2. 在**设置使用规则<规则名称>资产**对话框，选择您需要使用该规则的数据库。
3. 单击**确定**。

批量启用规则，操作步骤如下：

1. 在**规则管理**页面，定位到要批量启用的规则，选中其**等级**左侧的复选框。

   当选中规则**等级**左侧的复选框后，**规则列表**中的**启用全部**自动变更为**启用选中项**。

2. 单击**启用选中项**。
3. 在**选择资产**对话框，选择您需要启用该规则的数据库。
4. 单击**确定**。

启用全部规则，操作步骤如下：

1. 在**规则管理**页面，单击**启用全部**。
2. 在**选择资产**对话框，选择您需要启用全部规则的数据库。
3. 单击**确定**。

禁用规则与启用规则操作步骤相似，如您需要禁用规则，可以参考上述对应操作步骤取消启用、选择禁用选中项、选择禁用全部即可。

后续步骤

- 当目标数据库的审计记录命中启用的审计规则时，审计规则会触发告警。您可以查询数据库的告警信息。具体操作，请参见告警日志。
- 您可以配置用户规则中的白名单，满足白名单设置的审计记录，即使命中了用户规则，也不会触发告警。更多信息，请参见配置白名单。

11.2. 配置白名单

本文介绍了在云盾数据库审计系统中新增白名单和为用户规则设置白名单的具体操作。

背景信息

添加用户规则后，您可以启用用户规则，具体操作，请参见配置审计规则。当审计记录命中启用的用户规则时，用户规则会触发告警。

添加用户规则后，您可以为用户规则添加白名单设置。满足白名单设置的审计记录，即使命中了用户规则，也不会触发告警。

新增白名单

1. 登录云盾数据库审计系统。

   具体操作，请参见登录数据库审计系统。

2. 在左侧导航栏，选择**规则配置 > 安全规则**。
3. 单击**白名单管理**页签。
4. 在**白名单列表**中，单击**新增**。

5. 在**新增白名单**面板中，完成白名单配置。

名称：白名单的名称。

描述：白名单的描述信息。

白名单规则：具体的**客户端**、**服务端**、**行为**、**结果**、**其他**配置描述，请参见规则配置参数描述表格。

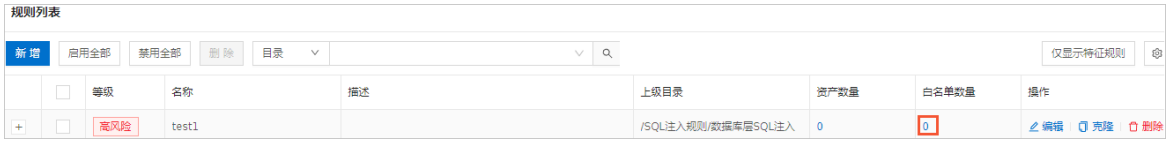
6. 单击**保存**。

成功添加白名单后，您可以在**白名单列表**中查看新添加的白名单，在白名单**操作**列下可以进行**编**

辑、**删除**操作。

为用户规则设置白名单

1. 在**安全规则**页面中，单击**规则管理**页签。
2. 定位到目标规则，单击**白名单数量**列下的数字。



3. 在**设置规则<规则名称>的白名单**对话框，根据您的需要，选择需要为该规则引用的白名单，将其**状态**更改为**启用**。

12.报表中心

报表中心功能支持使用多种报表类型展示数据库审计的分析结果。支持的报表类型包括塞班斯报表、综合分析报告、性能分析报表等，您可以根据业务需要使用对应的报表。本文介绍支持的报表类型，以及如何通过报表中心查看、订阅、导出报表和管理订阅任务。

支持的报表类型

报表名称	说明
塞班斯报表	本报表可以帮助管理人员、审计人员及时发现各种异常和违规行为，以便对这些行为进行快速分析、定位和响应，为整体信息安全管理提供决策依据。
综合分析报告	本报告从SQL语句执行情况分析、会话连接分析、风险事件分析和SQL性能分析四个角度对数据库进行综合分析。
性能分析报表	本报表在您指定的范围内从性能变化趋势、性能最差的数据库或SID、耗时最久的SQL、性能最差的SQL模板、执行最多的SQL模板五个方面对数据库的性能做出分析。
等保参考分析报表	本报表根据当前信息安全技术网络安全等级保护评测要求GB/T 28448-2019（简称等级保护2.0），针对等级保护2.0中关注的安全审计中的入侵防范、恶意代码监控、安全审计监控等进行针对性的数据分析和展示。
语句分析类报表	本类报表在您指定的范围内从SQL语句分析、失败语句分析、SQL语句变化趋势、审计趋势分析和执行次数最多SQL模板分析五个维度分析和展示当前语句类信息。
会话分析类报表	本类报表包含会话数量变化趋势分析、新增会话分析、并发会话分析和失败会话分析。
告警分析类报表	本类报表从告警变化趋势、告警来源分析、告警对象分析、规则命中分析四个维度分析当前告警的情况。
其他报表	本类报表包括客户端工具分析、数据库账号分析、数据库或SID分析、数据库访问来源IP分析。

查看、订阅和导出报表

1. 登录云盾数据库审计系统。

   具体操作，请参见登录数据库审计系统。
2. 在左侧导航栏，选择**报表中心 > 报表预览**。
3. 在**报表预览**页面，单击要查看的报表页签。

   报表中心支持多种报表类型，各报表类型的详细信息，请参见支持的报表类型。

4. 在报表内容上方，设置查询选项，查看报表内容。

   支持设置的查询选项包括以下内容：

   - **资产**：选择报表展示的资产和资产组。
   - **时间范围**：本日、本周、本月、最近3个月、最近6个月、最近12个月、昨天、上周、上个月、自定义。

     > **说明** 报表的统计粒度与设置的时间范围有关。
     >
     > - 时间范围小于24小时时，报表以小时为单位进行统计。
     > - 时间范围大于24小时且不足40天时，报表以天为单位进行统计。
     > - 时间范围大于40天时，报表以月为单位进行统计。

5. 订阅报表。

   订阅报表后，数据库审计服务会以邮件的形式定期向您发送该报表。参照以下步骤，添加一个报表订阅任务：

   i. 在当前报表右上角，单击**订阅**。

   ii. 在**添加订阅任务**面板，配置订阅任务的参数。

订阅任务的参数描述参见下表。

配置项	说明
任务名称	设置订阅任务的名称。
收件人邮箱	设置收件人的邮箱地址。支持填写多个邮箱地址，多个邮箱地址间以逗号（,）分隔。

配置项	说明
报表类型	选择要订阅的报表的类型，取值： ■ 塞班斯报表 ■ 综合分析报告 ■ 性能分析报表 ■ 等保参考分析报表 ■ SQL语句分析 ■ 失败语句分析 ■ SQL语句变化趋势分析 ■ 会话数量变化趋势分析 ■ 新增会话分析 ■ 并发会话分析 ■ 失败会话分析 ■ 告警趋势分析 ■ 告警来源分析 ■ 告警对象分析 ■ 规则命中分析 ■ 客户端工具分析 ■ 数据库账号分析 ■ 数据库/SID分析 ■ 数据库访问来源IP分析 ■ 审计趋势分析 ■ 执行次数最多SQL模板分析
报表格式	选择要订阅的报表的格式，取值： ■ HTML ■ PDF ■ PNG ■ WORD
资产	选择要订阅报表的数据库资产和资产组。
任务周期	订阅任务的邮件发送周期，取值： ■ 每天（日报） ■ 每周（周报） ■ 每月（月报） ■ 每年（年报）
发送时间	根据设置的任务周期，设置邮件发送的具体时间。

iii. 单击**保存**。

成功添加订阅任务后，如果您需要编辑或删除订阅任务，您可以在**管理订阅任务**页面进行相应操作。具体操作，请参见管理订阅任务。

6. 导出报表。

报表中心支持导出HTML、PDF、PNG和WORD格式的报表，您可以参考以下步骤导出所需格式的报表：

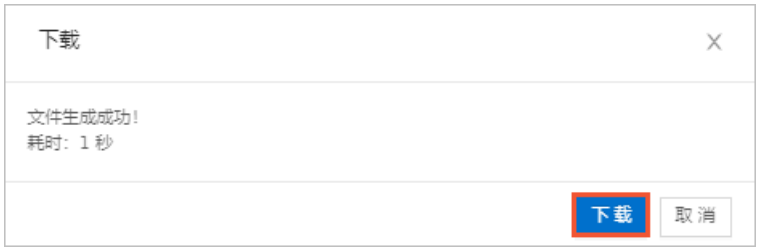
i. 在当前报表右上角，单击**导出**。

ii. 选择导出报表的格式。

支持选择以下格式：

- **HTML（推荐使用）**
- **PDF**
- **PNG**
- **WORD**

iii. 等待文件成功生成后，在**下载**对话框，单击**下载**。



当前报表文件会下载到本地您浏览器默认的下载路径下。

管理订阅任务

1. 登录云盾数据库审计系统。

具体操作，请参见登录数据库审计系统。

2. 在左侧导航栏，选择**报表中心 > 报表订阅**。

3. 在**管理订阅任务**页面，根据需要添加、编辑、删除订阅任务。

- 添加订阅任务
  a. 单击订阅任务列表上方的**添加**。
  b. 在**添加订阅任务**面板，完成订阅任务配置。添加订阅任务的参数描述详情，请参见配置说明。
  c. 单击**保存**。

  成功添加订阅任务后，已添加的订阅任务将显示在**订阅任务列表**中。数据库审计服务会定期向您指定的邮箱发送订阅的报表。
- 编辑订阅任务
  a. 在订阅任务列表中，定位到要编辑的订阅任务，单击其**操作**列的**编辑**。
  b. 在**编辑订阅任务**面板，修改订阅任务配置。订阅任务的参数描述详情，请参见配置说明。
  c. 单击**保存**。
- 删除订阅任务
  a. 在订阅任务列表中，定位到要删除的订阅任务，单击其**操作**列的**删除**。
  b. 在**确定删除订阅任务**对话框，单击**确定**。

  操作成功后，数据库审计服务将从订阅任务列表中删除该订阅任务，且后续不会向您的邮箱发送对应的报表。

13.管理Agent

数据库审计提供了Agent管理功能，使用该功能您可以设置Agent占用服务器资源的阈值，根据您的需要进行挂起、唤醒或停止Agent等操作。本文介绍管理Agent支持的具体操作。

前提条件

已在您的服务器中安装Agent。具体操作，请参见安装Agent。

修改Agent配置

数据库审计支持设置Agent的运行模式和数据审计抓包规则，比如CPU亲和性、最大CPU使用率、最大内存使用量、抓包网口等，您可以参考以下步骤修改Agent配置。

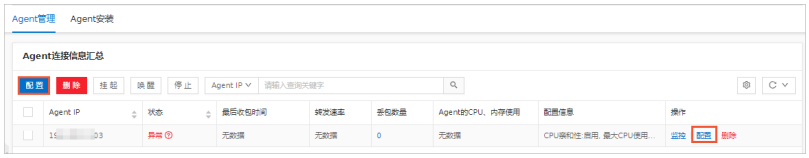
1. 登录数据库审计系统。

   具体操作，请参见登录数据库审计系统。

2. 在左侧导航栏，选择**系统管理 > Agent管理**。

3. 在**Agent管理**页签下，定位到需要配置的Agent，单击其**操作**列的**配置**。

   如果需要同时配置多个Agent，您可以选中多个Agent后，单击Agent列表上方的**配置**。



4. 在**修改Agent配置**对话框，参考以下表格配置Agent参数。

参数	说明
CPU亲和性	选择启用或禁用**CPU亲和性**。 启用CPU亲和性后，Agent将仅在单个CPU核心上工作。禁用CPU亲和性后，Agent将在多个CPU核心上工作，这种情况下可能会占用您较多的CPU资源。建议您启用**CPU亲和性**。
最大CPU使用率	设置最大CPU使用率。 Agent所占有的CPU使用率不会超过该设定值。如果该值设置过小，会导致审计数据不全面，建议您设置合理的值。

参数	说明
最大内存使用量	设置最大内存使用量。 Agent所占用的内存不会超过该设定值。如果该值设置过小，会导致审计数据不全面。建议您设置为200 MB。
CPU使用率阈值	设置CPU使用率阈值。 当服务器整体的CPU使用率超过该值时，Agent将停止工作。
内存使用率阈值	设置内存使用率阈值。 当服务器整体的内存使用率超过该值时，Agent将停止工作。
回环网口替换IP（IPv4）	设置本地回环的IPv4地址。 设置该地址后，数据库审计服务会将网络流量中本地回环的IPv4地址改为该地址。不设置此参数时，不做任何变更。
回环网口替换IP（IPv6）	设置本地回环的IPv6地址。 设置该地址后，数据库审计服务会将网络流量中本地回环的IPv6地址改为该地址。不设置此参数时，不做任何变更。
调试模式	选择启用或禁用调试模式。 启用调试模式后，数据库审计服务会记录更详细的调试日志。
抓包网口	设置需要抓取流量包的网口。多个网口请使用空格分隔。 设置该参数后，数据库审计服务只抓取您设置的网口上的流量。不设置此参数时，默认抓取全部网口上的流量。
回环网口	设置回环网口的名称。 不设置时会自动识别回环网口的名称。不建议您设置该参数。
抓包过滤串	设置抓包的过滤串。 配置后，数据库审计服务将不再根据配置的资产自动抓包，只在抓包网口抓取匹配该过滤串的流量。配置示例：`(host 192.168.1.100 and port 3306) or (host 192.168.1.101 and port 3306)`。
回环抓包过滤串	设置回环抓包过滤串。 配置后，将不再根据配置的资产自动抓包，只在回环网口抓取匹配该过滤串的流量。填写示例：`(port 3306) or (port 3307)`。

5. 单击**确定**。

查看Agent监控信息

数据库审计服务支持查看指定时间内已安装Agent的服务器CPU、内存使用情况，以及网口的转发速率和丢包数量等信息。您可以参考以下步骤查看Agent监控到的服务器数据：

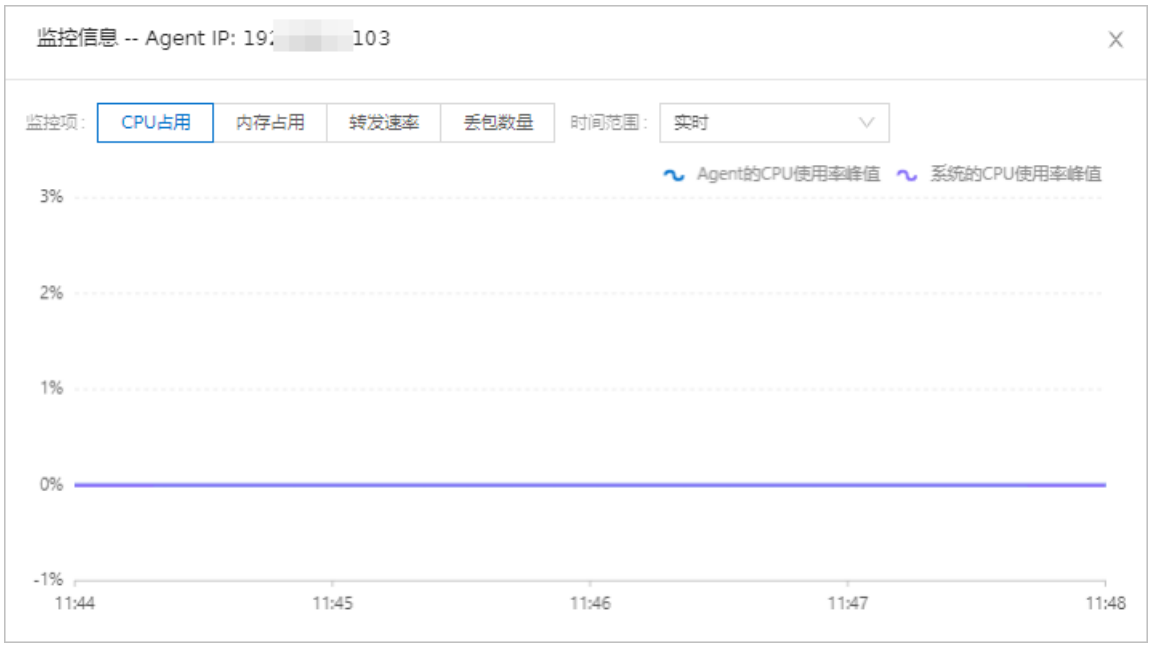
1. 登录数据库审计系统。

   具体操作，请参见登录数据库审计系统。

2. 在左侧导航栏，选择**系统管理 > Agent管理**。
3. 定位到需要查看监控信息的Agent，单击其**操作**列下的**监控**。
4. 在**监控信息**对话框，单击**CPU占用**、**内存占用**、**转发速率**或**丢包数量**页签，查看对应数据的趋势图。

   数据库审计默认为您展示实时的监控信息，您可以在**时间范围**下拉列表中选择需要查看的时间范围，支持选择：

   - **实时**
   - **最近30分钟**
   - **最近1小时**
   - **最近12小时**
   - **今天**
   - **昨天**
   - **本周**
   - **上周**



挂起、唤醒、停止、删除Agent

根据您使用场景的需要，您可以对Agent进行挂起、唤醒、停止、删除操作。您可以参考以下步骤执行具体操作。

1. 登录数据库审计系统。

   具体操作，请参见登录数据库审计系统。

2. 在左侧导航栏，选择**系统管理 > Agent管理**。
3. 定位到需要操作的Agent，参考以下说明挂起、唤醒、停止或删除Agent。

   - 挂起Agent

如果Agent所在服务器的CPU或内存资源消耗过大，您可以使用挂起功能停止Agent的工作。选中需要挂起的Agent，单击Agent列表上方的**挂起**。挂起Agent后，该Agent将停止转发数据库访问流量到审计系统等操作，但仍会和数据库系统保持通信连接。

> **注意** 只有状态为**正常**的Agent才能执行挂起操作。

- 唤醒Agent

  挂起Agent后，如果您需要Agent再次正常运行，可以使用唤醒功能，将**挂起**状态的Agent恢复正常运行。选中需要唤醒的Agent，单击Agent列表上方的**唤醒**。

- 停止Agent

  如果Agent所在服务器的CPU或内存资源消耗过大，或您暂时无需Agent转发您数据库的访问流量，您可以使用停止功能。您只能停止**挂起**或**正常**状态的Agent。选中需要停止的Agent，单击Agent列表上方的**停止**。停止Agent后，Agent会停止向数据库审计系统转发数据库的访问流量，并中断和数据库审计系统之间的网络连接。如果需要再次启用Agent，您需要在Agent所在服务器手动启用Agent。

- 删除Agent

  如果Agent处于**异常**状态或您无需再使用Agent转发数据库的访问流量，您可以删除Agent。选中需要删除的Agent，单击Agent列表上方的**删除**。您也可以定位到需要删除的Agent，单击其**操作**列下的**删除**。删除Agent后，该Agent将从Agent列表中移除。